Clipper meets Apple vs. FBI: a comparison of the cryptography discourses from 1993 and 2016

Schulze, Matthias

Veröffentlichungsversion / Published Version
Zeitschriftenartikel / journal article

Empfohlene Zitierung / Suggested Citation:
Schulze, M. (2017). Clipper meets Apple vs. FBI: a comparison of the cryptography discourses from 1993 and 2016. *Media and Communication*, *5*(1), 54-62. https://doi.org/10.17645/mac.v5i1.805

COGITATIO

Media and Communication (ISSN: 2183–2439)
2017, Volume 5, Issue 1, Pages 54–62
DOI: 10.17645/mac.v5i1.805

Article

Clipper Meets Apple vs. FBI—A Comparison of the Cryptography Discourses from 1993 and 2016

Matthias Schulze

International Relations Department, Friedrich-Schiller University Jena, 07743 Jena, Germany;
E-Mail: matthias.schulze@mailbox.org

Submitted: 31 October 2016 | Accepted: 18 January 2017 | Published: 22 March 2017

Abstract
This article analyzes two cryptography discourses dealing with the question of whether governments should be able to monitor secure and encrypted communication, for example via security vulnerabilities in cryptographic systems. The Clipper chip debate of 1993 and the FBI vs. Apple case of 2016 are analyzed to infer whether these discourses show similarities in their arguments and to draw lessons from them. The study is based on the securitization framework and analyzes the social construction of security threats in political discourses. The findings are that the arguments made by the proponents of exceptional access show major continuities between the two cases. In contrast, the arguments of the critics are more diverse. The critical arguments for stronger encryption remain highly relevant, especially in the context of the Snowden revelations. The article concludes that we need to adopt a more general cyber security perspective, considering the threat of cyber crime and state hacking, when debating whether the government should be able to weaken encryption.

Keywords
Apple; cryptowar; discourse analysis; encryption; FBI

Issue
This article is part of the issue "Post-Snowden Internet Policy", edited by Julia Pohle (WZB Berlin Social Science Center, Germany) and Leo Van Audenhove (Vrije Universiteit Brussel, Belgium).

1. Introduction

One effect of the leaks by former National Security Agency (NSA) contractor Edward Snowden in 2013 was that both Apple and Google introduced encryption to their smartphones. Law enforcement and intelligence agencies protested that widespread, unbreakable encryption would make it harder to retrieve evidence from these phones in criminal investigations (Kehl, Wilson, & Bankston, 2015, p. 1). In early 2016, the Federal Bureau of Investigation (FBI) issued a court order to compel Apple to unlock an encrypted iPhone 5C that was used by the San Bernardino attacker in December 2015. The FBI wanted Apple to rewrite its iOS software, to disable encryption security features that would allow the enforcement agency to guess the correct passcodes in a trial and error fashion. Apple resisted and ignited a wider debate within the context of the presidential elections. For some observers, the Apple/FBI debate resembled another instance of the so-called crypto-wars, defined as technological debates about whether the government should have access to encrypted communication. The crypto-wars between national security actors, technology firms and Internet users emerged during the early days of the World Wide Web in late 1992 with the debate about the Clipper chip (Kehl et al., 2015). The aim of this contribution is to analyze whether these two crypto-war discourses are in fact similar. Are there any lessons that can be drawn for the current debate?

This paper builds broadly on the Copenhagen School (Buzan, Waever, & Wilde, 1997) in International Relations and the concept of securitization of technology (Barnard-Wills & Ashenden, 2012; Deibert & Rohozinski, 2010; Hansen & Nissenbaum, 2009), which provides a link to Science and Technology Studies. Securitization is understood as the social construction of security/insecurity, for example in the digital realm (cyber security). Actors compete in the discourse over the mean-

ing of security, i.e. what counts as a threat and how these threats should be dealt with (Dunn Cavelty, 2013). Threat constructions are used for the legitimization of extraordinary security measures that would not be approved by a democratic audience in the absence of a threat. These measures include electronic surveillance, Internet censorship (Deibert, 2015), offensive computer-network-attack capabilities (Lawson, 2012) and exceptional access or state-regulation of encrypted communication, called crypto-politics (Moore & Rid, 2016).

Interestingly, the securitization framework has been rarely adopted to study cryptography discourses. Studies on the crypto-wars debate tend to be either technical (see Abelson et al., 2015; Dam & Lin, 1996) or historical (Kehl et al., 2015). Empirical securitization studies, which focus on digital technologies, tend to ignore the potential material impact of discourses, as Dunn Cavelty argues (Dunn Cavelty, 2015). The securitization of cryptography could have severe implications for cyber security but also for human rights in the digital age. Governmental access to otherwise secure cryptography could, in the worst case, substantially weaken these systems and thus threaten the safety of digital technologies like smartphones, which billions of people use.

The next section offers a short introduction to cryptography debates and outlines the two cases. These are then compared in a qualitative fashion, focusing on what the dominant arguments and actors are. I will concentrate on similarities first and then discuss the differences between the discourses. The final section offers a critical discussion of the arguments.

2. A Short History of the Crypto-Wars

Encryption is a century-old technique to scramble readable text, via mathematical algorithms, into unreadable cypher-text. Sender and recipient require a correct key or password to make the encrypted text intelligible again. The purpose of encryption is to avoid eavesdropping from third parties. Since 1976, a method called public-key encryption (Diffie & Hellman, 1976) promised easy-to-use, widespread encryption of electronic communication. The NSA recognized the potential danger to its global signals intelligence (interception of communication data) effort, if encrypted communication became a mainstream technology. Director of the NSA, Bobby Inman, warned that "unrestrained public discussion of cryptologic matters will seriously damage the ability of this government to conduct signals intelligence" (Inman, 1979, p. 130). Coinciding with the beginning of the personal computer revolution, the NSA argued that an important data source would be "going dark" if every new PC user were to use encrypted, digital communications. Thus, the entire sphere of digital communication could be metaphorically shrouded in darkness, unreadable to the NSA. The dilemma of how to resolve this issue was born.

In 1992, American Telephone and Telegraph (AT&T) began with the development of a consumer-market telephone that could encrypt voice communication between two parties. The NSA recognized that with the looming digital age, traditional, interceptable audio communication could be replaced by encrypted digital communication (Kaplan, 2016, p. 21). This led NSA Director Michael McConnell to rush into the development of the Clipper technology, which would set a standard for the emerging market. The proposal theoretically allowed user-friendly encryption based on a hardware chip called Clipper, which would be attached to devices like phones or computers. In contrast to other products on the market, it had a built-in security weakness: a copy of the encryption key would be stored in government databases. This key-escrow method gave law enforcement "exceptional access" to an otherwise secure technology. The NSA and FBI could thus eavesdrop on any Clipper-based phone call with a warrant because they could access a copy of the key. In February 1993, the newly elected Clinton–Gore Administration adopted the idea (Levy, 1994). On April 16th, 1993, the White House announced the launch of the voluntary Clipper initiative (White House, 1993). A strong public reaction across the political spectrum followed. Most computer experts, technology companies and a social movement of digital natives opposed it (Rid, 2016, pp. 333–337). A series of hearings were held to evaluate the technology. In early 1994, the Clipper program officially started, yet it never saw any widespread adoption. According to the National Research Council, only 10,000 to 15,000 Clipper-enabled phones have ever been sold, mostly to the government (Dam & Lin, 1996, p. 174). A CNN survey in 1994 found that roughly 80% of Americans opposed the initiative (US Senate, 1994). The death blow came when a cryptography expert discovered a security flaw within Clipper's algorithm, although the NSA and its supporters claimed the system was superior and more secure than anything else on the market (Brickel, Denning, Kent, Maher, & Tuchman, 1993). During the mid-1990s, the proposal was silently dropped. According to General Michael Hayden, the NSA "lost" this crypto-war: "We didn't get the Clipper Chip, we didn't get the back door" (Hayden, 2016a).

An outcome of the Clipper debate was that the US government relaxed its strict opposition to the widespread use of encryption. Laws like the Communications Assistance for Law Enforcement Act (CALEA) were adopted to prohibit the government from forcing companies to build government backdoors in their technology (Crawford, 2016). Over time, the US government relaxed its very strict export-regime that treated cryptographic products as dual-use goods. By the end of the 1990s, a widespread consensus (Kehl et al., 2015, p. 19) had been reached that "the advantages of more widespread use of cryptography outweigh the disadvantages" (Dam & Lin, 1996, p. 6). Scientists made the convincing case that key-escrow systems "enabling exceptional access to keys would be inherently less secure, more expensive, and much more complex than those without" (Abelson et al., 2015, p. 7).

The debate about governmental "exceptional access" reemerged in the summer of 2014, after Apple had decided to turn device encryption of its iPhones on by default. On October 10th, FBI Director James B. Comey warned that encryption was hindering evidence retrieval for law enforcement. Comey urged the government to adopt a legislative fix and companies to find a solution (Comey, 2014). In fall 2015, the Washington Post published internal communication from within the intelligence community complaining about a hostile legislative environment on the encryption matter "that could turn in the event of a terrorist attack or criminal event where strong encryption can be shown to have hindered law enforcement" (Nakashima & Peterson, 2015). This was a reference to President Obama who had indicated that his government would not pursue legislation on the matter. The debate resurfaced on February 16th, 2016, when an US Magistrate ruled—ex parte—that Apple must provide "reasonable technical assistance" to FBI investigators to unlock an iPhone 5C that belonged to the San Bernardino shooter of December 2015 (Volz & Menn, 2016). The judge issued the warrant based on the All Writs Act (AWA) from 1789, which becomes active only if there is no other governing law, thus bypassing CALEA (Tangri, Lemley, Feldman, & Landers, 2016). Apple indeed helped the FBI with this iPhone, but mistakes were made and normal unlocking procedures did not work. Apple CEO Tim Cook, the main protagonist of the counter-discourse, contested that the court order was "unreasonably burdensome" (Cook, 2016a). Because of the ongoing election campaign, multiple high profile politicians, intelligence professionals, media and tech companies began to publicly take side with or against Apple. According to a Pew survey, the public sided with the FBI initially, with around 51% arguing that Apple should help the FBI. However, later polls with diverse methodologies showed that the public sided with Apple (Elmer-Dewitt, 2016). The fierce discourse about encryption lasted until March, when a Brooklyn court ruled in Apple's favor that AWA did not govern the unlocking of an iPhone in a similar case (Lichtblau & Goldstein, 2016). The whole debate suddenly disappeared in March, when it became public that a third party could unlock the iPhone without Apple's help (Benner & Apuzzo, 2016). Two weeks later it was revealed that the phone did not include any valuable information (McGoogan, 2016) and the Department of Justice issued a filing that it would no longer need Apple's assistance (Novet, 2016).

3. Methodology

The paper analyses the Clipper discourse between 1993–1994 and the Apple/FBI case between 2014 and 2016, with a focus on the peak of the debate in February/March 2016. Using the snowball technique, a literature corpus (Apple/FBI N = 42, Clipper N = 22) was assembled that contains official statements, newspaper or internet coverage, congressional hearings and some scientific literature of the respective debates. Documents repeatedly mentioned in the corpus were analyzed more deeply using content analysis techniques (Mayring, 2000). The first step was to identify the different discursive positions (opponents, proponents and middle ground). Then the arguments of the respective positions were inductively identified and coded throughout the corpus in an iterative fashion (Keller, 2007). Some codes were deduced from the securitization framework, namely *threats*, *threatened referent* objects and *extraordinary measures* that are demanded to remedy the threat and that go beyond established social norms and procedures (Buzan et al., 1997, pp. 23–24). Another aim was to find out which characteristics, whether negative or positive, were being attributed to encryption. Finally, the frequencies of individual codes were counted and collected in a table to provide some (limited) quantitative insights and to assess what the most dominant arguments were in each debate. Of course, these findings are not generalizable and serve more as an ideal type (Weber, 1973) to gauge the general content of other potential cryptography discourses in the future.

During the Clipper discourse in 1993, only 27% of Americans owned a computer and 2% used the Internet (World Bank, 2016). The Apple/FBI discourse on the other hand happened at a time when 87% of Americans used the Internet (World Bank, 2016), 73% had a computer and 68% a smartphone (Anderson, 2015). In contrast to 1993, cyber security issues like hacking, data theft and state-sponsored cyber attacks were ubiquitous in 2016, with encryption being one line of defense against these issues. This means that in 2016, potentially more customers were affected by the encryption debate. Additionally, the Apple/FBI case stands in the context of the Snowden leaks of 2013 which uncovered the extensive Internet surveillance capacities of the NSA and its targeted operations against encryption systems. NSA programs like Bullrun allegedly implanted software backdoors in HTTPS encryption used for secure web-browsing and also utilized hardware backdoors for exceptional access to Internet routers (Ball, Borger, & Greenwald, 2013). Other Snowden leaks indicate intense NSA efforts to gain access to encrypted Virtual Private Network connections, often used by large corporations to offer secure access to files from afar (Goodin, 2015), or even the Onion Router or TOR network, that utilizes multiple layers of encryption and thus is highly resistant to eavesdropping (Sayer, 2014). Thus, the Snowden leaks increased public awareness of data security, encryption and concerns about government surveillance programs (Rainie & Maniam, 2016).

4. Comparing Two Crypto-War Discourses

4.1. Similarities between Clipper and Apple vs. FBI

The discursive positions in the two discourses are somewhat similar. Law enforcement (FBI), intelligence actors

(NSA) and politicians (predominantly, but not exclusively conservatives) argue for governmental regulation of encryption and providing exceptional access for legitimate law enforcement inquiries. In both discourses, this group produces a relatively homogenous set of arguments. Technology companies, cryptography experts, scientists and a mix of civil-libertarians and tech enthusiasts argue for widespread, public use of encryption. This group is more heterogeneous and uses a huge variety of arguments. In both instances, there is a middle ground, recognizing the needs of both groups and arguing for a compromise (which is technologically difficult to achieve).

When comparing the two discourses, it becomes immediately obvious that the law enforcement perspective is very similar in both cases. The general argument is that "encryption threatens to significantly curtail, and in many instances, preclude, effective law enforcement" (Sessions, 1993), which resembles the NSA's warning from 1979. This is the main argument (uttered 27x) within the debate and a center-piece of the "going dark" metaphor. It is supported by and often combined with a legalistic justification that with a court order or a warrant, the government should have access to encrypted communication (39x). This is the extraordinary measure demanded. It is extraordinary in the sense, that the government wants access to communication intended for no-one else except the communicating parties and demands from companies to change their technology to meet wiretapping needs, effectively influencing hard and software development (Lessig, 2006, p. 66). In other words, the crypto-war discourse is about establishing/contesting the norm of government control over cryptography vs. the right of every user to communicate privately (Levy, 1994).

How are these extraordinary capabilities and powers legitimized? Proponents argue that "criminals" (27x) and "terrorists" (31x) cannot be caught if they use encryption. Interestingly, the Clipper discourses highlights "drug-traffickers", whereas the Apple/FBI discourse is more about "terrorists" and "child molesters". These are framed by law enforcement as the main threats. Closely connected to the argument is the frame that "law enforcement must keep pace" (9x) with malign actors. It creates the impression that the highly trained and equipped, multi-million dollar law enforcement apparatus is falling behind. The referent objects that need to be protected from these threats are mentioned in statements like the following: "Successful conduct of electronic surveillance is crucial to effective law enforcement, to the preservation of the public safety, and to the maintenance of the national security" (15x) (Sessions, 1993). This clearly indicates a national-security perspective. Widespread encryption itself is presented as a threat or at least as a problem to national security (7x). The key description here is that encryption is presented (10x) as a "dual-edge sword: encryption helps to protect the privacy of individuals and industry, but it also can shield criminals and terrorists" (White House, 1993). The dilemma is that in both cases, the government recognizes the positive effects of encryption for privacy and the protection of intellectual property (12x). Therefore, the key metaphor is the demand for the rightful balance between privacy and (national) security (11x). In sum, the negative effects of encryption and threats to national security outweigh the benefits. The argument can be found in its entirety in the press release following the official announcement of the Clipper initiative in 1994: "if encryption technology is made freely available worldwide, it would no doubt be used extensively by terrorists, drug dealers, and other criminals to harm Americans both in the US and abroad. For this reason, the Administration will continue to restrict export of the most sophisticated encryption devices, both to preserve our own foreign intelligence gathering capability and because of the concerns of our allies who fear that strong encryption technology would inhibit their law enforcement capabilities" (White House, 1994).

Whereas the government predominantly uses national security-related arguments, the counter-discourse is more heterogeneous. There are three types of argument. Technical arguments state that government access makes encryption systems less secure and are mostly put forward by the technology and science community. Economic arguments argue against government interference in the market and the costs of the proposal. Finally, there are civil liberty arguments that revolve around privacy and mistrust of the expansion of state power and are uttered by libertarians. There are also several other arguments that overlap or do not necessarily fall into either group. Their common denominator is that the government wants to interfere with the products of private companies (24x) in terms of hardware with Clipper and software with Apple. The metaphor of choice is that the government wants to create a "backdoor" (25x) in an otherwise secure system. Libertarians see this as an expansion of government authority, or with the words of Apple CEO Tim Cook as "government overreach" (20x) and thus as a potential threat (Cook, 2016a). Business actors are more afraid of the potential future effects of the government regulating encryption, which might result in the widespread use of inferior technology (15x).

These diverse groups share a relatively similar perspective on encryption. Cryptography is a privacy-enhancing technology (19x) and seen in an exclusively positive way (13x). This explains why any government interference is seen as problematic. The referent objects in this discourse are privacy and civil liberties in particular (24x) and, more implicitly, American identity and values, which are prominently present in the Apple/FBI discourse. The argument in both cases is that control of encryption technology is a norm of authoritarian regimes and police states and therefore inappropriate in democracies (14x). The technological principles of encryption must be understood to make sense of this frame. The fewer parties have access to a system, the more secure it gets. Ideally, public key encryption only has two parties,

the sender and receiver. With key-escrow, a third party (the government) is introduced, which creates security risks. The threat in both cases is that the method for exceptional access could fall into the wrong hands (21x) and thus could potentially be misused. In the case of Clipper, the key-escrow database could be stolen, and with the Apple/FBI case, the source code for bypassing iOS security could be hacked, for example by foreign states.

However, there is also a general critique against the government mandating which encryption products to use. In both discourses, technical experts point to the fact that those with malign interest will find a way around government mandated encryption (17x). The key question that comes up in congressional hearings is: Which bad actor would use a technology that he/she knows the government is using to listen in (12x)? Ultimately, law-abiding citizens would be forced to use an inferior technology, while bad actors could use encryption without US backdoors from the international market. This argument is particularly brought forward by critics in the Apple/FBI case (11x), but also existed in a slightly different form in 1993. The reference to foreign crypto-products or the "off-shoring" of cryptography, as former Director of NSA Michael Hayden calls it, is a compelling argument in both cases (Hayden, 2016b). It creates the overall risk that cryptography evolves outside the US market where the government has even less control. This would create a competitive disadvantage for American tech firms. The economic damage of regulating cryptography to American business is a key argument in the Clipper discourse (21x), but not so much in the Apple/FBI case (1x).

The general argument put forward by critics in both cases is that the government should look at the bigger picture (33x), recognizing the general interest of the people and corporations that need encryption, both for privacy reasons but also for business interests and data security. Cryptography is no longer a state monopoly but a matter for citizens (5x) and therefore the government should not prioritize the particular interests of the NSA and FBI. In other words, the general positive effects outweigh the negative effects for a greater audience. This ultimately reflects the legal and discursive consensus that was reached during the mid-1990s.

4.2. Differences

Clipper and the Apple vs. FBI cases differ in some aspects. The Clipper initiative is a government attempt at standard-setting using a NSA-developed chip. It is also a voluntary technology initiative and not a law per se. This means that the government utilizes a range of arguments to "sell" their product to the skeptical audience by arguing Clipper is far superior to anything else on the market (22x), that Clipper does not weaken, but enhances, privacy (9x) and generally that Clipper strikes the right balance between security and privacy (6x). These arguments are particularly highlighted in White House briefing documents from the FBI/NSA and indicate that the Clinton–Gore Administration must have been aware of a potential backlash (Sessions, 1993). Another indicator for this anticipation is the fact that this initiative is not a law, but described as a "voluntary" tech initiative (7x).

Critics contest these arguments. The tech community argues that the NSA developed Clipper (7x) and its encryption algorithm in secrecy (11x), which goes against industry best practices of public code evaluation and the law because the National Institute for Standards would be legally in charge (9x). Others criticize the enormous cost of several million dollars annually that it would take just to maintain the key-escrow infrastructure and the cost of the Clipper chip itself, which would increase hardware prices (8x). Because of these technical facts, the initiative is described as premature, rushed and not thought through (9x). A CNN poll of the time indicates that a majority of 80% is not convinced of the government's arguments (US Senate, 1994). The fact that almost all technology companies and experts are against the Clipper initiative is an important point (17x). To understand this, one must consider the strong skepticism vis a vis government interference in the market (12x).

This is different in the counter-terrorism and post-Snowden context of 2016. The first theme of the Apple vs. FBI discourse is that encryption and its potential weakening is not about the singular San Bernardino case but a *general matter*. Apple systematically argues that government mandated exceptional access is a "threat to millions of customers worldwide" and not just in the US (30x). For Apple, the debate is not about one particular iPhone, but a general case that affects potentially every phone today and in the future (40x). The FBI wants to interfere with Apple's hard/software design (24x) to mandate the construction of a backdoor (25x). Apple calls it the "software equivalent of cancer" (Cook, 2016b). If the courts allowed this, it would create a dangerous legal precedent (26x), which the FBI repeatedly denies (although Comey testifies that the FBI has around 600 other iPhones to be unlocked) (C-Span, 2016). Apple repeatedly argues that in the encryption debate we need to look at the bigger picture, beyond law enforcement interests (33x). The bigger picture includes the cyber security landscapes and new threats: from cyber attacks (20x), data-theft (14x) and hackers (15x). Backdoors resemble weaker encryption which itself is represented as a threat (19x). Backdoors would introduce vulnerabilities to all iPhones, which would represent an enormous public safety risk (16x) because iPhones are used in areas like government agencies and critical infrastructures. These areas would become vulnerable to hacking. Weak encryption would make the entire digital infrastructure less secure (10x). Apple also fears a potential future spillover: weakening encryption now will harm the US digital infrastructure in the future (9x), because exploits could be stolen, and thus fall into the wrong hands (15x). The powerful technical argument that there is no backdoor that could be exploited just by the good guys is put forward (11x). Moreover, other agencies might dig up cases to

mandate companies to build in backdoors for more trivial reasons than fighting terrorism, a phenomenon called function creep (10x).

The second discursive feature is an identity or moral narrative. Apple argues that the referent objects are not just millions of customers or privacy and civil liberties but American identity in general (23). "This is not who we are", says Tim Cook (Cook, 2016b). If Western Democracies follow authoritarian regimes in their control of private communication (via government access), it would create a soft-power precedent (10x). Dictatorships would feel legitimized in their surveillance of citizens. Likewise, the FBI uses moralizing statements like "It is about the victims and justice. Fourteen people were slaughtered and many more had their lives and bodies ruined….We can't look the survivors in the eye, or ourselves in the mirror, if we don't follow this lead" (Comey, 2016b). However, most of the FBI's argument is rather legalistic, focusing on the argument that there should be no "warrant-proof" spaces (Comey, 2016a).

In sum, the FBI and Apple recognize each other's good intentions and need for cooperation to resolve this problem. Both parties argue that there needs to be a broad public discussion about this difficult issue (22x). Policymakers in general favor strong encryption with exceptional, warrant-based access while the tech community replies that the mathematics either support secure encryption without government backdoors or exceptional access with significantly less security. The combination of both secure cryptography and governmental access represents wishful thinking or the search for a magic pony solution (Abelson et al., 2015).

5. Discussion

Whereas the Clipper discourse is focused mostly on the privacy/security dichotomy, the Apple/FBI case shows that in times of cyber crime and hacking, this dichotomy needs to be rethought. Traditionally, the two have been framed as an antagonism or a zero-sum game: more security means less privacy/liberty. This is not necessarily true anymore because encryption enhances both privacy and security, both individually but also collectively or globally. In an interconnected world, a vulnerability in one iPhone is a threat for every user, as the recent Pegasus spyware, which affected all 1 billion active iOS devices, shows. Encryption is crucial for the security of digital infrastructures (i.e. cyber security). The question we need to address is "whose security are we talking about"? The debate shows that there are two paradigms of security at work: a national security perspective with traditional, physical threats such as terrorism and a cyber security perspective, which considers the vulnerabilities of software and hardware in terms of hacking, cyber crime and state-sponsored cyber war. Former NSA Director Michael Hayden belongs to the latter and argues that considering the cyber threat, "America is simply more secure with unbreakable end-to-end encryption" (Hayden, 2016a).

The second element we need to discuss critically is the "going dark" metaphor, which creates a false dualism of light and shadow and thus another artificial zero-sum game. The metaphor ignores the fact that there are multiple sources of light. Wiretapping of conversations is just one stream of data among an increasing number of law enforcement tools like automated biometric recognition, DNA sampling, geo-location tracking or contact-chaining with social network analysis. Our "digital exhaust" as Michael Hayden calls it, the often unencrypted metadata we generate using smartphones and online services such as Facebook or Google, is in fact growing (Hayden, 2016b). Never before has there been so much private information about us in the open. The government has access to most of these new sources of data. The amount of data traversing global networks in 2016 makes the year 1993 appear like the dark ages of data and law enforcement. Arguing that we are currently "in the light" and the future will be dark is somewhat misleading. Just because content data is increasingly more encrypted and one channel of data collection might be "going dark", it does not mean that all other channels are going dark as well. The opposite is probably true.

The "going dark" metaphor creates a false technological-deterministic assumption that widespread cryptography will *automatically* lead to only one single outcome: a future of uninterceptable information. This scenario is unlikely. There is no such thing as unbreakable encryption. It might get more complicated but it is unlikely that it will ever be impossible to break. Even today, strong cryptography is circumvented by exploiting other weaknesses in the system, which probably is the reason why the FBI got into the San Bernardino iPhone without Apple's help (Benner & Apuzzo, 2016). Even if encryption was unbreakable, it would not be guaranteed that it would ever reach 100% user adoption. The technological barriers for users are still high and market mechanisms like ad-based, big-data business models stand in the way of widespread adoption. Practical reasons prohibit the adoption of encryption, which is the same reason why we do not whisper all the time to avoid eavesdropping. It is often too impractical and inconvenient. Even if everyone used encryption, people often make mistakes with the implementation which makes their systems vulnerable to attack (Gasser et al., 2016, p. 3).

Determinism overstates the effects of technology and ignores human response strategies. It is too easy to blame technologies when old strategies fail. To blame technology would be akin to the French blaming the invention of the tank for their inferior defense strategy against the German Blitzkrieg tactics in World War 2. There are always two components: technology and human agency. If encryption is indeed a problem, then law enforcement and intelligence agencies simply must adapt and change their operating strategies (Landau, 2016). For example, if electronic surveillance of a drug dealer is not feasible anymore because he/she uses encrypted phone calls, one way to resolve the problem

would be to use human intelligence like surveillance personnel on the ground or even traditional acoustic surveillance bugs implanted in a car or house. Particularly the "Internet of Things (IoT)" with microphones in Smart TVs and loudspeakers and the trend of cloud-computing will offer new, unique capabilities that could be used in the traditional warrant process (Gasser et al., 2016, p. 10). At the same time, in the context of the growing vulnerabilities of a digitalized IoT infrastructure, safe systems and strong encryption are imperative. The old Clipper consensus that the widespread use of cryptography is the greater good is still valid, even though it is understandably harder to see in the current context of global terrorism.

As threatening as terrorism may be, cyber attacks from nation-states, cyber crime and digital espionage are growing rapidly and are costing millions of dollars annually. Richard C. Clarke, the senior counter-terrorism official during the Bush administration argued: "my point is encryption and privacy are larger issues than fighting terrorism" (Clarke, 2016). The ongoing securitization of cryptography in liberal democracies sets a normative precedent. Directly after the Apple/FBI debate, countries like Russia began to demand backdoors in cryptographic messengers like WhatsApp and Telegram by law and referred to the practices of Western democracies for justification (Howell O'Neill, 2016). Currently, France, Great Britain, Germany and others are pursuing similar legislation. Interestingly, the discourses in liberal and authoritarian countries rely on similar rhetorical figures, threat descriptions and referent objects identified in this article. To qualify this, further comparative research would be required. Authoritarian regimes will probably use exceptional access not to prosecute terrorists, but the political opposition or human rights NGOs. Besides this normative argument there is also a technical one: the more governments replicate this practice of actively punching holes in cryptography without disclosing them publicly, the less secure the worldwide IT-infrastructure gets.

Acknowledgements

Thanks to the anonymous reviewers for their positive and constructive feedback.

Conflict of Interests

The author declares no conflict of interests.

References

Abelson, H., Anderson, R., Bellovin, S. M., Benalo, J., Blaze, M., Diffie, W., . . . Weitzner, D. J. (2015). *Keys under doormats: Mandating insecurity by requiring government access to all data and communications* (Computer Science and Artificial Intelligence Laboratory Technical Report, MIT-CSAIL-TR-2015-026). Cambridge, MA: Massachusetts Institute of Technology.

Anderson, M. (2015). Technology device ownership: 2015. *Pew Research Center*. Retrieved from http://www.pewinternet.org/2015/10/29/technology-device-ownership-2015

Ball, J., Borger, J., & Greenwald, G. (2013). Revealed: How US and UK spy agencies defeat internet privacy and security. *The Guardian*. Retrieved from https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

Barnard-Wills, D., & Ashenden, D. (2012). Securing virtual space: Cyber war, cyber terror, and risk. *Space and Culture*, *15*(2), 110–123.

Benner, K., & Apuzzo, M. (2016). US says it may not need Apple's help to unlock iPhone. *The New York Times*. Retrieved from http://nyti.ms/1UzGJTS

Brickel, E. F., Denning, D. E., Kent, S. T., Maher, D. P., & Tuchman, W. (1993). *Skipjack review: Interim report* (The SKIPJACK Algoritm). Retrieved from https://epic.org/crypto/clipper/skipjack_interim_review.html

Buzan, B., Waever, O., & Wilde, J. D. (1997). *Security: A new framework for analysis*. London: Lynne Rienner Publishers Inc.

C-Span. (2016). Apple iPhone encryption hearing. *C-Span*. Retrieved from https://www.c-span.org/video/?405442-1/hearing-encryption-federal-investigations

Clarke, R. (2016). Encryption, privacy are larger issues than fighting terrorism, Clarke says. *NPR.prg*. Retrieved from http://www.npr.org/2016/03/14/470347719/encryption-and-privacy-are-larger-issues-than-fighting-terrorism-clarke-says

Comey, J. (2014). Going dark: Are technology, privacy, and public safety on a collision course? *US Department of Justice*. Retrieved from https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course

Comey, J. (2016a). Encryption tightrope: Balancing Americans' security and privacy. *US Department of Justice*. Retrieved from https://www.fbi.gov/news/testimony/encryption-tightrope-balancing-americans-security-and-privacy

Comey, J. (2016b). FBI director comments on San Bernadino matter. *US Department of Justice*. Retrieved from https://www.fbi.gov/news/pressrel/press-releases/fbi-director-comments-on-san-bernardino-matter

Cook, T. (2016a). *A message to our customers*. Retrieved from http://www.apple.com/customer-letter

Cook, T. (2016b). Apple CEO Tim Cook sits down with David Muir. *ABC News*. Retrieved from http://abcnews.go.com/WNT/video/exclusive-apple-ceo-tim-cook-sits-david-muir-37174976

Crawford, S. (2016). The law is clear: The FBI cannot make Apple rewrite its OS. *Backchannel*. Retrieved from https://backchannel.com/the-law-is-clear-the-fbi-cannot-make-apple-rewrite-its-os-9ae60c3bbc7b#.sa125j16z

Dam, K. W., & Lin, H. S. (1996). *Cryptography's role in securing the information society*. Washington, DC: National Research Council.

Deibert, R. J. (2015). Cyberspace under siege. *Journal of Democracy*, *26*(3), 64–78.

Deibert, R. J., & Rohozinski, R. (2010). Risking security: Policies and paradoxes of cyberspace security. *International Political Sociology*, *4*(1), 15–32.

Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, *22*(6), 644–654.

Dunn Cavelty, M. (2013). From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse. *International Studies Review*, *15*(1), 105–122.

Dunn Cavelty, M. (2015). Die materiellen Ursachen des Cyberkriegs Cybersicherheitspolitik jenseits diskursiver Erklärungen. *Journal of Self-Regulation and Regulation*, *1*, 167–184.

Elmer-Dewitt, P. (2016). Apple vs. FBI: What the polls are saying. *Fortune*. Retrieved from http://fortune.com/2016/02/23/apple-fbi-poll-pew

Gasser, U., Gertner, N., Goldsmith, J., Landau, S., Nye, J., O'Brien, D. R., . . . Zittrain, J. (2016). *Don't panic. Making progress on the "Going Dark" debate*. Cambridge, MA: Berkman Klein Center.

Goodin, D. (2015). How the NSA can break trillions of encrypted Web and VPN connections. Researchers show how mass decryption is well within the NSA's $11 billion budget. *Ars Technica*. Retrieved from http://arstechnica.com/security/2015/10/how-the-nsa-can-break-trillions-of-encrypted-web-and-vpn-connections

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. *International Studies Quarterly*, *53*, 1155–1175.

Hayden, M. V. (2016a). Hayden: The pros and cons of access to encrypted files. *Youtube*. Retrieved from https://www.youtube.com/watch?v=6HNnVcp6NYA

Hayden, M. V. (2016b). General Michael Hayden on the Apple FBI and data encryption. *AEIdeas*. Retrieved from https://www.aei.org/publication/gen-michael-hayden-on-apple-the-fbi-and-data-encryption

Howell O'Neill, P. (2016). Russia lawmakers pass sweeping spying law that requires encryption backdoors, call surveillance. *The Daily Dot*. Retrieved from http://www.dailydot.com/layer8/encryption-backdoor-russia-fsb-bill-passes

Inman, B. R. (1979). The NSA perspective on telecommunications protection in the nongovernmental sector. *Cryptologia*, *3*, 129–135.

Kaplan, F. (2016). *Dark territory: The secret history of cyber war*. New York, NY: Simon & Schuster.

Kehl, D., Wilson, A., & Bankston, K. S. (2015, June). *Doomed to repeat history? Lessons from the crypto wars of the 1990s* (Report from the New America Foundation). Washington, DC: New America.

Keller, R. (2007). *Diskursforschung*. Berlin: Springer.

Landau, S. (2016). The real security issues of the iPhone case. Law enforcement needs 21st-century investigative savvy. *Sciencemag*, *352*(6292), 1398–1399.

Lawson, S. (2012). Putting the "war" in cyberwar: Metaphor, analogy, and cybersecurity discourse in the United States. *First Monday*, *17*(7). doi:10.5210/fm.v17i7.3848

Lessig, L. (2006). *Code: And other laws of cyberspace, version 2.0*. New York, NY: Basic Books.

Levy, S. (1994). Battle of the Clipper chip. *The New York Times*. Retrieved from http://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html

Lichtblau, E., & Goldstein, J. (2016). Justice Dept. appeals ruling in Apple iPhone case in Brooklyn. *The New York Times*. Retrieved from https://www.nytimes.com/2016/03/08/technology/justice-dept-appeals-ruling-in-apple-iphone-case-in-brooklyn.html

Mayring, P. (2000). Qualitative content analysis. *Forum: Qualitative Sozialforschung*, *1*(2). Retrieved from http://www.qualitative-research.net/index.php/fqs/article/view/1089

McGoogan, C. (2016). Terrorist's iPhone didn't turn up any useful information, FBI admits. *The Telegraph*. Retrieved from http://www.telegraph.co.uk/technology/2016/04/15/terrorists-iphone-didnt-turn-up-any-useful-information-fbi-admit

Moore, D., & Rid, T. (2016). Cryptopolitik and the darknet. *Survival*, *58*(1), 7–38.

Nakashima, E., & Peterson, A. (2015). Obama faces growing momentum to support widespread encryption. *Washington Post*. Retrieved from https://www.washingtonpost.com/world/national-security/tech-trade-agencies-push-to-disavow-law-requiring-decryption-of-phones/2015/09/16/1fca5f72-5adf-11e5-b38e-06883aacba64_story.html

Novet, J. (2016). Apple vs. FBI: A timeline of the iPhone encryption case. *VB*. Retrieved from http://venturebeat.com/2016/02/19/apple-fbi-timeline

Rainie, L., & Maniam, S. (2016). Americans feel the tensions between privacy and security concerns. *Pew Research Center*. Retrieved from http://www.pewresearch.org/fact-tank/2016/02/19/americans-feel-the-tensions-between-privacy-and-security-concerns

Rid, T. (2016). *Maschinendämmerung: Eine kurze Geschichte der Kybernetik*. Berlin: Propyläen Verlag.

Sayer, P. (2014). Snowden docs show Tor, TrueCrypt, Tails topped NSA's 'most wanted' list in '12. *Computerworld*. Retrieved from http://www.computerworld.com/article/2863937/snowden-docs-show-tor-truecrypt-tails-topped-nsas-most-wanted-list-in-12.html

US Senate. (1994). *The administration's clipper chip key escrow encryption program: Hearing before the Subcommittee on Technology and the Law of the Committee on the Judiciary United States Senate*, Washington, DC: US Senate.

Sessions, W. S. (1993). *Leaked letter briefing document "Encryption: The threat, applications, and potential solutions"*. Retrieved from https://epic.org/crypto/clipper/foia/crypto_threat_2_19_93.html

Tangri, D., Lemley, M. A., Feldman, M. A., & Landers, A. L. (2016). Amicus Curiae Brief of law pro-

fessors in support of Apple Inc. *Apple*. Retrieved from http://www.apple.com/pr/library/2016/03/03Amicus-Briefs-in-Support-of-Apple.html

Volz, D., & Menn, J. (2016). Apple ordered to help FBI unlock data from San Bernadino shooter's iPhone. *Reuters*. Retrieved from http:// www.reuters.com/article/california-shooting-timcook-idUSKCN0VQ0YG

Weber, M. (1973). Die "Objektivität" sozialwissenschaftlicher und sozialpolitischer Erkenntnis. In J. Winckelmann (Ed.), *Gesammelte Aufsätze zur Wissenschaftslehre* (pp. 146–214). Tübingen: Mohr.

White House. (1993). *Statement by the press Secretary*. Retrieved from https://epic.org/crypto/clipper/white_house_statement_4_93.html

White House. (1994). *Statement by the press Secretary*. Retrieved from https://epic.org/crypto/clipper/white_house_statement_2_94.html

WorldBank. (2016). Internet users (per 100 people). *World Bank*. Retrieved from http://data.worldbank.org/indicator/IT.NET.USER.P2

About the Author

Matthias Schulze, MA, is a political scientist working on issues such as surveillance (data retention) and cyber security (encryption) and cyber war in both democratic and authoritarian states. In his PhD thesis, he analyzes normative change in the behavior of democratic states towards the Internet, represented by increased surveillance and cyber war practices and discourses.